

SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

COMMUNICATION SYSTEM, INTERCONNECTING DEVICE AND PROGRAM FOR AUTHENTICATING A USER OF A COMMUNICATION NETWORK

Cross Reference to Related Applications

This patent application claims priority from a Japanese patent application No. 2002-041305 filed on February 19, 2002, the contents of which are incorporated herein by reference.

Background of Invention

Field of the Invention

[0001] The present invention relates to a communication system, an interconnecting device and a computer program. More particularly, the present invention relates to authentication of a communication network user to prevent improper or unauthorized use of a communication line by a user.

Description of the Related Art

[0002] With recent widespread home use of the Internet, it is expected that high-speed lines, e.g., broadband, capable of delivering a large volume of data, such as audio data, image data and movie data, via the Internet will be realized. In response to such demand, ADSL (Asymmetric Digital Subscriber Line), FTTH (Fiber To The Home) and the like have been offered to users who access the Internet via routers that can handle PPPoE (Point to Point over Ethernet) connections.

[0003] A conventional router that handles a PPPoE connection stores a user name and a password, which typically are set by a user, and access to the Internet, or other dedicated network, is obtained by transmitting the user name and password to an authentication apparatus of an Internet service provider in accordance with the user's instruction. Therefore, the conventional router has a problem or potential security problem in that the user's communication line, which is accessed by the router, may be used improperly by any user, whether authorized or not, by merely connecting through the router since the conventional router can access the communication line in accordance with the instruction of any user based upon the user name and password previously stored therein.

Summary of Invention

[0004] Therefore, it is an object of the present invention to provide a communication system, an interconnecting device and a program stored in a computer-readable medium, which are capable of overcoming the above drawbacks accompanying the conventional art. The above and other objects can be achieved by combinations described in the independent claims. The dependent claims define further advantageous and exemplary combinations of the present invention.

[0005] According to a first aspect of the present invention, a communication system, that connects a first network and a second network for communication thereof, includes a first interconnecting device connected to a first communication device of the first network; a second interconnecting device, connected to the first interconnecting device and a second communication device of the second network, and operable to control whether or not communication between the first and second communication devices is allowed; and an external recording device operable to store authentication information of a user of the first communication device. The authentication information being used for authentication of the user by the second interconnecting device. The first interconnecting device includes an acquiring unit operable to acquire the authentication information of the user of the first communication device from the external recording device; and a transmit unit operable to transmit the authentication information acquired by the acquiring unit to the second interconnecting device.

[0006] The second interconnecting device includes a receive unit operable to receive the

authentication information from the first interconnecting device; an authentication unit operable to authenticate the authentication information received by the receive unit; and a setting unit operable to set the second interconnecting device to allow the communication between the first and second communication devices, in a case where the authentication by the authentication unit was successful.

[0007] The acquiring unit of the first interconnecting device is further operable to acquire bandwidth information from the external recording device; the transmit unit of the first interconnecting device is further operable to transmit the bandwidth information acquired by the acquiring unit to the second interconnecting device; the receive unit of the second interconnecting device is further operable to receive the bandwidth information from the first interconnecting device; and the setting unit of the second interconnecting device is further operable to set a bandwidth of the communication between the first and second communication devices based on the bandwidth information received by the receive unit.

[0008] According to a second aspect of the present invention, an interconnecting device, for connecting a first network and a second network to enable communication between a first communication device of the first network and a second communication device of the second network, includes an acquiring unit operable to acquire from a recording device, which is outside the interconnecting device, authentication information of a user of the first communication device for authentication of the user, by an authentication apparatus, for controlling whether or not communication between the first and second communication devices is allowed; and a transmit unit operable to transmit the authentication information received by the acquiring unit to the authentication apparatus.

[0009] The acquiring unit includes a reading unit operable to read the authentication information from a non-volatile memory, as the recording device, storing the authentication information.

[0010] The acquiring unit includes a receive unit operable to perform wireless communication with a wireless communication device, as the recording device, storing the authentication information, and to receive the authentication information from the wireless communication device by the wireless communication.

[0011] The acquiring unit further acquires identification information of the authentication apparatus from the recording device, and the transmit unit transmits the authentication information acquired by the acquiring unit to the authentication apparatus identified by the identification information acquired by the acquiring unit.

[0012] The interconnecting device includes a setting unit operable to set a bandwidth of the communication between the first and second communication devices. The acquiring unit further acquires bandwidth information from the recording device, and the setting unit sets the bandwidth of the communication between the first and second communication devices based on the bandwidth information acquired by the acquiring unit.

[0013] The interconnecting device includes a decryption unit operable to decrypt encrypted authentication information in a case where the acquiring unit acquires the authentication information after encryption.

[0014] The interconnecting device includes a processing unit operable to determine whether or not the authentication apparatus is allowed to authenticate the user. The transmit unit transmits the authentication information acquired by the acquiring unit to the authentication apparatus when the processing unit determines that the authentication apparatus is allowed to authenticate the user.

[0015] The processing unit determines that the authentication apparatus is allowed to authenticate the user when the first communication device has been turned on.

[0016] The processing unit determines that the authentication apparatus is allowed to authenticate the user when the interconnecting device has been turned on.

[0017] According to a third aspect of the present invention, a program, stored in a computer-readable medium, for use in an interconnecting device that connects a first network and a second network to allow communication between a first communication device of the first network and a second communication device of the second network, includes an acquiring unit operable to acquire from a recording device, that is outside the interconnecting device, authentication information of a user of the first communication device, used for authentication of the user by an authentication apparatus for controlling whether or not communication between the

first and second communication devices is allowed; and a transmit unit operable to transmit the authentication information to the authentication apparatus.

[0018] The program includes a setting unit operable to set a bandwidth of the communication between the first and second communication devices. The acquiring unit further operates to acquire bandwidth information from the recording device, and the setting unit operates to set the bandwidth of the communication between the first and second communication devices based on the bandwidth information.

[0019] The program includes a decryption unit operable to decrypt encrypted authentication information when the authentication information is encrypted.

[0020] The summary of the invention does not necessarily describe all necessary features of the present invention. The present invention may also be a sub-combination of the features described above. The above and other features and advantages of the present invention will become more apparent from the following description of the embodiments taken in conjunction with the accompanying drawings.

Brief Description of Drawings

[0021] Fig. 1 illustrates an exemplary structure of a communication system 100 according to an embodiment of the present invention.

[0022] Fig. 2 illustrates a first exemplary structure of an interconnecting device 10a according to one embodiment of the present invention.

[0023] Fig. 3 illustrates a second exemplary structure of an interconnecting device 10a according to one embodiment of the present invention.

[0024] Fig. 4 illustrates an exemplary structure of an interconnecting device 40 according to one embodiment of the present invention.

[0025] Fig. 5 shows an operation flow of the communication system 100 according to one embodiment of the present invention.

[0026] Fig. 6 illustrates a hardware configuration of PC 20a according to one embodiment of the present invention.

Detailed Description

[0027] The invention will now be described based on the preferred embodiments, which do not intend to limit the scope of the present invention, but exemplify the invention. All of the features and the combinations thereof described in the embodiments are not necessarily essential to the invention.

[0028] Fig. 1 illustrates an exemplary structure of a communication system 100 according to an embodiment of the present invention. The communication system 100 includes interconnecting devices 10a and 10b; recording devices 15a and 15b; personal computers (PCs) 20a, 22a, 20b and 22b, as examples of communication devices; an interconnecting device 40; a network 50, such as the Internet; a server 60, such as a Web server; and a server 62, such as a mail server. The interconnecting device 10a connects PCs 20a and 22a to the interconnecting device 40. The interconnecting device 10b connects PCs 20b and 22b to the interconnecting device 40. The interconnecting device 40 connects the interconnecting devices 10a and 10b to the network 50, e.g., the Internet.

[0029] PCs 20a and 22a form LAN 30a while PCs 20b and 22b form LAN 30b. LANs 30a and 30b are an exemplary first network according to one embodiment of the present invention. The network 50 is an exemplary second network according to one embodiment of the present invention. Moreover, PCs 20a, 22a, 20b and 22b are examples of the first communication device according to one embodiment of the present invention. The server 60 and the server 62 are exemplary second communication devices according to one embodiment of the present invention. The interconnecting device 40 serves as an example of an authentication apparatus according to one embodiment of the present invention.

[0030] The recording device 15a stores authentication information used for authentication, by the interconnecting device 40, of a user of the interconnecting device 10a (i.e., a user of PC(s) 20a and/or 22a). The recording device 15a provides the authentication information to the interconnecting device 10a. Also, the recording device 15b stores authentication information used for authentication of a user of the interconnecting device 10b (i.e., a user of PC(s) 20b and/or 22b) by the interconnecting device 40, and provides the authentication information to the

interconnecting device 10b. The recording devices 15a and 15b may be a non-volatile memory, such as an IC card, a miniature card, or a floppy disk, or a wireless communication device capable of performing wireless communication, such as IrDA. Moreover, it is desirable that the recording devices 15a and 15b store encrypted authentication information.

[0031] The interconnecting device 10a obtains the authentication information to be used for authentication of the user of the interconnecting device 10a, by the interconnecting device 40, from the recording device 15a. The interconnecting device 10a then transmits the authentication information to the interconnecting device 40 in accordance with a user's instruction in order to connect LAN 30a to the Internet network 50. Similarly, the interconnecting device 10b obtains the authentication information to be used for authentication of the user of the interconnecting device 10b, by the interconnecting device 40, from the recording device 15b. The interconnecting device 10b then transmits the authentication information to the interconnecting device 40 in accordance with a user's instruction in order to connect LAN 30b to the Internet network 50.

[0032] For example, in an embodiment where the interconnecting devices 10a and 10b are connected to the interconnecting device 40 by PPPoE connection, each of the interconnecting devices 10a and 10b acquires a name and a password of the corresponding user as the authentication information from the associated recording device 15a or 15b and then transmits the acquired information to the interconnecting device 40. In another embodiment where the interconnecting devices 10a and 10b are connected to the interconnecting device 40 by dial-up connection, each of the interconnecting devices 10a and 10b acquires a destination phone number, the user name and the password as the authentication information from the associated recording device 15a or 15b and then transmits the acquired authentication information to the interconnecting device 40.

[0033] The interconnecting device 40 controls whether or not the interconnecting devices 10a and 10b are connected to the Internet network 50. In other words, the interconnecting device 40 controls whether or not communication is allowed between each of PCs 20a, 22a, 20b and 22b and the Web server 60 and mail server 62.

[0034] The interconnecting device 40 authenticates the authentication information received from the interconnecting device 10a or 10b. In a case where authentication of the information received from the interconnecting device 10a was successful, the interconnecting device 40 enables communication between LAN 30a and the Internet network 50. Thus, PCs 20a and 22a of LAN 30a can be connected to the Internet network 50 and therefore the user(s) of PCs 20a and 22a can use the Web server 60 and the mail server 62. Also, the interconnecting device 40 enables communication between LAN 30b and the Internet network 50 in a case where authentication of the information received from the interconnecting device 10b was successful. Thus, PCs 20b and 22b can be connected to the Internet network 50 and therefore the user(s) of PCs 20b and 22b can use the Web server 60 and the mail server 62.

[0035] In the above description, the interconnecting device 40 authenticates only the authentication information received from the interconnecting devices 10a and 10b. However, the present invention is not limited thereto. The authentication may be performed by an external authentication apparatus connected to the interconnecting device 40. Moreover, the interconnecting device 40 and the external authentication apparatus may be connected directly to each other so as to allow communication there between, or may communicate with each other via the Internet network 50.

[0036] An Internet provider for managing the interconnecting device 40 provides the user, who signed up with the Internet provider for a communication line, with the interconnecting device 10a and the recording device 15a as a package or set, or the interconnecting device 10b and the recording device 15b as a package or set. The recording device 15a stores authentication information encrypted by the Internet provider, while the associated interconnecting device 10a has a decryption key used for decrypting the authentication information stored in the recording device 15a. Similarly, the recording device 15b stores authentication information encrypted by the Internet provider, while the associated interconnecting device 10b has a decryption key used for decrypting the authentication information stored in the recording device 15b.

[0037] Thus, only the user who owns (i.e., possesses) the recording device 15a can access the Internet network 50 by means of the interconnecting device 10a. Similarly,

only the user who owns (i.e., has possession of) the recording device 15b can access the Internet network 50 by means of the interconnecting device 10b. More specifically, the user of PC 20a or 22a owns, as a key for accessing the Internet network 50 via the interconnecting device 10a, the recording device 15a that stores authentication information for the user of the interconnecting device 10a. The user can access the Internet network 50 by using PC 20a or 22a by causing the interconnecting device 10a to acquire the authentication information stored in the recording device 15a. Similarly, the user of PC 20b or 22b owns, as a key for accessing the Internet network 50 via the interconnecting device 10b, the recording device 15b that stores authentication information for the user of the interconnecting device 10b. The user can access the Internet network 50 by using PC 20b or 22b by causing the interconnecting device 10b to acquire the authentication information stored in the recording device 15b. Moreover, since the recording devices 15a and 15b store the authentication information after being encrypted, disclosure or loss of the user's authentication information can be prevented.

[0038] According to the communication system 100 of the present embodiment, only the user who owns the recording device 15a can access the Internet network 50 via the interconnecting device 10a. Thus, it is possible to prevent an unfair use of the communication line by a user other than the user who owns the recording device 15a (that is, the user of the interconnecting device 10a who signed up for the communication line). Similarly, since only the user who owns the recording device 15b can access the Internet network 50 via the interconnecting device 10b, an unfair use of the communication line by a user other than the user who owns the recording device 15b (that is, the user of the interconnecting device 10b who signed up for the communication line) can be prevented.

[0039] Fig. 2 illustrates a first example of the structure of the interconnecting device 10a according to one embodiment of the present invention. The interconnecting device 10b has the same structure as the interconnecting device 10a and therefore only the interconnecting device 10a is described as a typical example.

[0040] The interconnecting device 10a of the first example of the present embodiment includes: a reading unit 102 serving as an exemplary acquiring unit operable to

acquire authentication information for allowing the interconnecting device 40 to authenticate the user of the interconnecting device 10a; a decryption unit 104 operable to decrypt the encrypted authentication information; a setting unit 106 operable to perform various settings related to communication in the interconnecting device 10a; a transmit/receive unit 108 operable to transmit data to the interconnecting device 40 and receive data from the interconnecting device 40; a transmit/receive unit 110 operable to transmit data to PCs 20a and 22a and receive data from PCs 20a and 22a; and a processing unit 112 operable to determine whether or not the authentication of the user of the interconnecting device 10a by the interconnecting device 40 is allowed.

[0041] The reading unit 102 holds the recording device 15a inserted thereto by the user of the interconnecting device 10a, that is a non-volatile memory, such as an IC card, a miniature card or a floppy disk, for storing authentication information of the user of the interconnecting device 10a. The reading unit 102 then reads out the authentication information from the non-volatile memory serving as the recording device 15a. The decryption unit 104 decrypts the authentication information read by the reading unit 102 in a case where the authentication information thus read was encrypted. The external transmit/receive unit 108 then transmits the authentication information decrypted by the decryption unit 104 to the interconnecting device 40.

[0042] The processing unit 112 determines whether or not the interconnecting device 40 is allowed to authenticate the user of the interconnecting device 10a. In other words, the processing unit 112 determines whether or not the transmission of the authentication information by the transmit/receive unit 108 is allowed. More specifically, the processing unit 112 may detect whether or not PC 20a or 22a which is connected to the transmit/receive unit 110 has been turned on, so as to allow the authentication of the user of the interconnecting device 10a by the interconnecting device 40 in a case where it was detected that PC 20a or 22a had been turned on.

[0043] Moreover, the processing unit 112 may detect whether or not the interconnecting device 10a has been turned on, so as to allow the authentication of the user of the interconnecting device 10a by the interconnecting device 40 in a case where it was detected that the interconnecting device 10a had been turned on.

[0044] Furthermore, the processing unit 112 may detect whether or not the transmit/receive unit 110 received a packet from PC 20a or 22a, so as to allow the authentication of the user of the interconnecting device 10a by the interconnecting device 40 in a case where the transmit/receive unit 110 received the packet. In this case, the transmit/receive unit 108 may transmit the authentication information read by the reading unit 102 from the recording device 15a, that is the non-volatile memory, to the interconnecting device 40.

[0045] The reading unit 102 may further read identification information of the interconnecting device 40 from the recording device 15a, which may be a non-volatile memory. In this case, the transmit/receive unit 108 may transmit the authentication information read from the recording device 15a to the interconnecting device 40 that is identified by the identification information read from the recording device 15a. In this way, it is possible to easily access any of a plurality of interconnecting devices 40 (that is, a plurality of Internet providers) by means of a single interconnecting device 10a, thus allowing change of the Internet provider depending on the service type of the communication line.

[0046] The reading unit 102 may further read from the recording device 15a, which may be a non-volatile memory, bandwidth information that describes a bandwidth in which the interconnecting device 10a can communicate with the interconnecting device 40. In this case, the setting unit 106 may set the bandwidth of communication between PCs 20a and 22a and the interconnecting device 40, that is, the bandwidth that can be used for communication between PCs 20a and 22a and the Web server 60 and mail server 62, based on the bandwidth information read by the reading unit 102 from the recording device 15a. More specifically, the setting unit 106 may limit the bandwidth of the communication between the interconnecting device 40 and the transmit/receive unit 108 of the interconnecting device 10a or the bandwidth of the communication between PCs 20a and 22a and the transmit/receive unit 110 of the interconnecting device 10a. Thus, the manager of the interconnecting device 40 (that is, the Internet provider) can easily set the bandwidth of communication that can be used by the user of the interconnecting device 10a. Moreover, the transmit/receive unit 108 may transmit the bandwidth information read by the reading unit 102 from the recording device 15a, to the interconnecting device 40.

[0047] Fig. 3 illustrates a second example of the interconnecting device 10a of the present embodiment. The same components as those in the first exemplary interconnecting device 10a shown in Fig. 2 are labeled with the same reference numerals. In addition, a description of the same structure and operations as those in the first example shown in Fig. 2 is partially omitted, and the structure and operations that are different from those in the first example shown in Fig. 2 are particularly described below.

[0048] The interconnecting device 10a according to the second example of the present embodiment includes a wireless communication unit 103 in place of the reading unit 102 of the first exemplary interconnecting device 10a. The wireless communication unit 103 receives, by wireless communication, authentication information of the user of the interconnecting device 10a from the recording device 15a, which may be a wireless communication device storing the authentication information. The wireless communication unit 103 may further read identification information of the interconnecting device 40 from the recording device 15a.

[0049] Fig. 4 illustrates an exemplary structure of the interconnecting device 40 of the present embodiment. The interconnecting device 40 includes an authentication unit 204 operable to perform authentication of the user of the interconnecting device 10a, a transmit/receive unit 206 operable to transmit data to the interconnecting device 10a and receive data from the interconnecting device 10a, a transmit/receive unit 200 operable to transmit data to the Internet network 50 and receive data from the Internet network 50, and a setting unit 202 operable to perform various settings related to communication in the interconnecting device 40.

[0050] The transmit/receive unit 206 receives authentication information of the user from the interconnecting device 10a. The authentication unit 204 then performs authentication for the authentication information received by the transmit/receive unit 206 from the interconnecting device 10a. In a case where the authentication was successful, the setting unit 202 sets the interconnecting device 40 to permit communication between the interconnecting device 10a and the Internet network 50.

[0051] The transmit/receive unit 206 may further receive bandwidth information from the interconnecting device 10a. In this case, the setting unit 202 may set the bandwidth of

the communication between the interconnecting device 10a and the Internet network 50, that is, the bandwidth of communication between the PCs 20a and 22a and the Web server 60 and mail server 62, based on the bandwidth information received by the transmit/receive unit 206. More specifically, the setting unit 202 may limit the bandwidth of the communication at a port of the transmit/receive unit 206 to which the interconnecting device 10a is connected. In this way, the manager of the interconnecting device 40 (that is, the Internet provider) can easily set the bandwidth of the communication used by the user of the interconnecting device 10a.

[0052] Fig. 5 shows an exemplary operation flow of the communication system 100 according to the present embodiment. First, in the interconnecting device 10a, the reading unit 102 shown in Fig. 2 or the wireless communication unit 103 shown in Fig. 3 acquires encrypted authentication information and bandwidth information from the recording device 15a (Step S100). The decryption unit 104 decrypts the authentication information acquired from the recording device 15a (Step S102). The processing unit 112 monitors whether or not PC 20a or 22a has been turned on (Step S104). In a case where PC 20a or 22a is on, the transmit/receive unit 108 transmits the authentication information to the interconnecting device 40 (Step S106).

[0053] Then, in the interconnecting device 40, the transmit/receive unit 206 receives the authentication information transmitted from the interconnecting device 10a (Step S200). The authentication unit 204 performs authentication for the authentication information received by the transmit/receive unit 206 (Step S202). In a case where the authentication by the authentication unit 206 was not successful (Step S203-N), the interconnecting device 40 does not permit the communication between the interconnecting device 10a and the Internet network 50, and the operation flow of the communication system 100 is finished. In another case where the authentication by the authentication unit 206 was successful (Step S203-Y), the setting unit 202 sets the interconnecting device 40 to allow the communication between the interconnecting device 10a and the Internet network 50 (Step S204). The transmit/receive unit 206 then notifies the interconnecting device 10a that the authentication was successful by transmitting information describing that fact (Step S205).

[0054] Next, in the interconnecting device 10a, the transmit/receive unit 108 transmits the bandwidth information to the interconnecting device 40 (Step S108). In the interconnecting device 40, the transmit/receive unit 206 receives the bandwidth information transmitted from the interconnecting device 10a (Step S206). The setting unit 202 then sets the bandwidth of the communication between the interconnecting device 10a and the Internet network 50 based on the bandwidth information received by the transmit/receive unit 206 (Step S208). Thus, PCs 20a and 22a can communicate with the Web server 60 and mail server 62 through the Internet network 50. In this way, the operation flow of the communication system 100 is finished.

[0055] Fig. 6 illustrates an exemplary hardware configuration of PC 20a according to one embodiment of the present invention. PC 20a includes a CPU 700, a ROM 702, a RAM 704, a communication interface 706, a hard disk drive 708, a database interface 710, a floppy disk drive 712 and a CD-ROM drive 714. CPU 700 operates based on at least one program stored in the ROM 702 and/or RAM 704. The communication interface 706 communicates with the interconnecting device 10a through a computer network, for example. The database interface 710 writes data into a database and updates the contents of the database.

[0056] The floppy disk drive 712 reads data or program from a floppy disk 720 to provide the read data or program to the communication interface 706. The CD-ROM drive 714 reads data or program from a CD-ROM 722 to provide the read data or program to the communication interface 706. The communication interface 706 transmits the data or program provided by the floppy disk drive 712 or CD-ROM drive 714 to the interconnecting device 10a. The database interface 710 can be connected to various types of database 724 to perform data transmission and data receiving therewith.

[0057] The program provided to the interconnecting device 10a is provided by a user while being stored in a recording medium such as the floppy disk 720 or the CD-ROM 722. The program stored in the recording medium may be compressed or not-compressed. The program is read from the recording medium to be installed into the interconnecting device 10a via the communication interface 706, so that the interconnecting device 10a executes the program.

[0058] The program provided while being stored in the recording medium, that is the program to be installed into the interconnecting device 10a, makes the interconnecting device 10a serve as a reading unit, a wireless communication unit, a decryption unit, a setting unit, a first transmit/receive unit, a second transmit/receive unit and a processing unit. The functions of the respective units are the same as the operations of the corresponding units in the interconnecting device 10a described referring to Figs. 1-3 and 5, and therefore a description is omitted here.

[0059] A part or all of the functions and operations of the interconnecting device 10a according to all the embodiments described herein can be stored in the floppy disk 720 or the CD-ROM 722 shown in Fig. 6 as examples of the recording medium.

[0060] These programs may be read directly into the interconnecting device 10a from the recording medium to be executed therein, or may be executed in the interconnecting device 10a after the programs are installed into the interconnecting device 10a. Moreover, the above-mentioned programs may be stored in a single recording medium or a plurality of recording media. Furthermore, the programs may be stored while being encoded.

[0061] As a recording medium, other than the floppy disk and the CD-ROM, an optical recording medium such as a DVD or a PD, a magneto-optical recording medium such as an MD, a tape-like medium, a magnetic recording medium, or a semiconductor memory, such as an IC card or a miniature card, can be used. Moreover, a storage device such as a hard disk or a RAM provided in a server system connected to an exclusive communication network or the Internet may be used as the recording medium, so that the program can be provided to the interconnecting device 10a through a communication network.

[0062] According to the present invention as described above, improper use of a network by a user who does not have possession of authentication information, which is stored in an external recording medium, can be prevented.

[0063] Although the present invention has been described by way of exemplary embodiments, it should be understood that those skilled in the art might make many changes and substitutions without departing from the spirit and the scope of the

present invention which is defined only by the appended claims.